Finite Geometries with Qubit Operators

Ambar N. Sengupta
Department of Mathematics, Louisiana State University,
Baton Rouge, LA 70803, USA
sengupta@math.lsu.edu

Received (Day Month Year)
Revised (Day Month Year)
Communicated by (xxxxxxxxxx)

Finite projective geometries, especially the Fano plane, have been observed to arise in the context of certain quantum gate operators. We use Clifford algebras to explain why these geometries, both planar and higher dimensional, appear in the context of multi-qubit composite systems.

AMS Subject Classification: 81Q99, 51E

Keywords: Projective Geometry, Qubits, Quantum Computing

1. Introduction

Finite projective geometries have appeared in several investigations relating to quantum computing; for example, Levay et al. [3], Rau [4], and Saniga et al. [5]. In this paper we present a mathematical explanation for the appearance of these geometries. We show that finite geometries arise from units in Clifford algebras which form a vector space over the field \( \mathbb{Z}_2 \) of two elements.

In quantum computing, the classical switch is replaced by its quantum counterpart, for which there is an observable \( S \) which takes values in \( \{0, 1\} \) and, moreover, the proposition ‘\( S \) takes the specific value 1’ and its negation are both minimal in the logic of propositions. The quantum switch is thus a system whose quantum Hilbert space \( \mathcal{H} \) is two-dimensional; the observable \( S \) is described by a self-adjoint operator on \( \mathcal{H} \), which has a basis \( |0\rangle, |1\rangle \), where \( |\lambda\rangle \) is a unit eigenvector for \( S \) with eigenvalue \( \lambda \). For instance, \( S \) could describe spin of a spin-half particle in a given direction. A qubit is a pure state of the switch system, and may be described by a unit vector in \( \mathcal{H} \). A composite system of switches is described by a suitable tensor power \( \mathcal{H} \otimes \cdots \otimes \mathcal{H} \), and a pure state of the composite system of the form \( |\lambda_1 \cdots \lambda_n\rangle \) encodes the bit string \( \lambda_1 \cdots \lambda_n \). In this quantum setting, a logic gate is a device that takes as input a multiqubit state \( |\lambda_1 \cdots \lambda_n\rangle \), applies an operator on \( \mathcal{H} \otimes \cdots \otimes \mathcal{H} \) and issues an output state on which measurements can be made. Of special interest are operators of the form \( \sigma_{j_1} \otimes \cdots \otimes \sigma_{j_n} \), where the \( \sigma_j \) are Pauli operators on \( \mathcal{H} \simeq \mathbb{C}^2 \).
described below in \((2.1)\). As we explain later in section \(2\) it is these operators which give rise to certain finite geometries.

There are intriguing relations between notions in quantum computing and aspects of black hole physics. Very briefly, black hole solutions to certain supersymmetric field theories are associated with parameters ranging over of certain (matrix) algebras; the Bekenstein-Hawking entropy of a black hole, which is proportional to the ‘surface area’ of the black hole, can be expressed in terms of algebraic invariants, such as the classical Cayley hyperdeterminant, of the parameters. Remarkably, by identifying the parameters with suitable operators on \(H \otimes n\), the algebraic invariant turns out to be related to entanglement measures of states of a composite quantum switch system. This then leads to relationship with finite geometries. We refer to Lévay et al.\(^3\) and references therein, for more on this.

As noted before there are several works where finite geometries have been observed to arise in the context of quantum computing. We refer to the online resource of Saniga\(^6\) where many such works are listed. Havlicek\(^2\) has also discussed a mathematical explanation for the appearance of these geometries, but does not use Clifford algebras. Our work is closest to and inspired by the work of Rau\(^4\).

\[2\] Appearance of Finite Geometries

First let us briefly recall that a projective geometry is specified by a set \(\mathcal{P}\) of points, a set \(\mathcal{L}\) of lines, an incidence relation \(I \subset \mathcal{P} \times \mathcal{L}\) (for which we say that a point \(A\) lies on a line \(l\), or that \(l\) passes through \(A\), if \((A, l) \in I\)) such that the following hold: (i) for every pair of distinct points \(A, B \in \mathcal{P}\) there is a unique line denoted \(AB\) which passes through \(A\) and \(B\); (ii) if \(A, B, C, D\) are points such that the lines \(AB\) and \(CD\) have a point in common, then the lines \(AC\) and \(BD\) also have a point in common; (iii) every line passes through at least three points. A set of points are collinear if they lie on a common line; a set of lines are coincident if they pass through a common point. A triangle is simply a set of three distinct points.

Under additional geometric hypotheses, the axioms (i)-(iii) can be used to construct a field \(k\) and a vector space \(V\) over \(k\) such that points correspond to one-dimensional subspaces of \(V\), lines to two-dimensional subspaces of \(V\), and incidence corresponds to the subspace relation. For any vector space \(V\), this specifies a projective geometry \(\mathbb{P}(V)\), which has a special feature called the Desargues property: if \(ABC\) and \(A'B'C'\) are triangles such that there is a point \(D\) which, for each \(X \in \{A, B, C\}\), is collinear with \(X\) and \(X'\), then there is a line \(l\) which, for every pair of distinct points \(X, Y \in \{A, B, C\}\), is coincident with the lines \(XY\) and \(X'Y'\). This is illustrated in Figure\(\square\).

Returning to ideas in quantum computing, most basic quantum gates are constructed from two-state systems, i.e. those with two-dimensional Hilbert spaces. The composite of such systems is described by tensor products of the corresponding Hilbert spaces. On choosing a fixed orthonormal basis \(|0\rangle\) and \(|1\rangle\) in the two-dimensional Hilbert space, we can identify this space with \(\mathbb{C}^2\). Some of the basic
quantum gates are expressed using tensor products of the Pauli matrices

\[
\sigma_1 = \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad\sigma_2 = \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad\sigma_3 = \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}
\]

(2.1)
along with the identity matrix \(\sigma_0 = I\). The Pauli matrices have zero trace, are hermitian as well as unitary, and form a basis of the three-dimensional real vector space of all zero-trace \(2 \times 2\) hermitian matrices; along with \(\sigma_0\), their real-linear span is the space of all hermitian matrices, and their complex linear span is the space of all \(2 \times 2\) complex matrices.

Let \(N\) be a fixed positive integer; we will work with gates which process \(N\) qubits, i.e. systems with state Hilbert space being \((\mathbb{C}^2)^{\otimes N}\). Let \(S\) be the set of all products of the \(N\)-fold tensor products of the matrices \(\sigma_\alpha\) with \(\alpha \in \{0, 1, 2, 3\}\).

Consider now a geometry constructed as follows. Points are the elements of \(S\), other than just the identity \(I\) and also \(-I\), with \(x\) and \(-x\) identified. Lines contain three points, with points \(a, b, c\) being on a line if \(ab\) equals \(\pm c\). Rau[4] shows (among other results) that for \(N \in \{1, 2\}\), this results in a projective space, and, furthermore, the Desargues property holds in this space. A variety of other such observations have been made by Levay et al[3].

In particular, consider the special case \(N = 1\). In this case, there are seven points, three corresponding to the Pauli matrices \(\sigma_j\), the three pairwise products \(\sigma_j\sigma_k\), with \(j \neq k\), and the triple product \(\sigma_1\sigma_2\sigma_3\). Thus, one can view this projective space in terms of a triangle with the Pauli matrices as vertices, with the point corresponding to \(\sigma_j\sigma_k\) (with \(j \neq k\)) lying on the line joining the vertices for \(\sigma_j\).
Ambar N. Sengupta

and $\sigma_k$, and a centroid-style point in the interior of the triangle, corresponding to $\sigma_1\sigma_2\sigma_3$. This space is called the Fano plane (see Figure 2). As Rau [4] points out, it also appears as a subspace of the projective space associated to the $N=2$ system. The appearance of the Fano plane in quantum computing related contexts has been noted in many works, including Rau [4], Levay [3] (and see the many works listed at [3]).

3. Finite Geometries from Clifford Algebras

In this section we shall explain why the finite projective geometries, satisfying the Desargues property, described in the preceding section arise.

The usual Clifford algebra $\mathbb{C}l_m$ over $m$ generators $e_1,...,e_m$ is the associative complex algebra with identity generated by these elements, along with an identity element $I$, subject to the relations

$$e_je_k + e_ke_j = 2\delta_{jk}I$$

for all $j, k \in \{1,...,m\}$.

Note that the square of each $e_j$ is $I$. This algebra (for a construction see Artin [1]) has dimension $2^m$, and a basis is formed by the products

$$e_S = e_{s_1}...e_{s_r},$$

for all subsets $S = \{s_1,...,s_r\}$, with $s_1 < s_2 < \cdots < s_r$, of $\{1,...,m\}$; the element $I = e_\emptyset$ is the multiplicative identity. The product is given by

$$e_{ST} = \epsilon_{ST}e_{S\Delta T},$$

where $S\Delta T$ is the set of elements in $S \cup T$ which are not in $S \cap T$, and $\epsilon_{ST}$ is the product of all $\epsilon_{st}$, with $s \in S$ and $t \in T$, where $\epsilon_{st} = -1$ if $s > t$ and $\epsilon_{st} = 1$ if $s \leq t$.

The Clifford algebra is a superalgebra, splitting into a sum of even and odd elements:

$$\mathbb{C}l_m = \mathbb{C}l_m^0 \oplus \mathbb{C}l_m^1,$$

where $\mathbb{C}l_m^0$ is spanned by products of even numbers of the elements $e_j$, and $\mathbb{C}l_m^1$ spanned by products of odd numbers of elements. It is important to note that here we are working with the Clifford algebra, not a representation of it; for example, with $m = 3$, if we consider the representation of $\mathbb{C}l_3$ using Pauli matrices, $\sigma_1\sigma_2$ is equal to $i\sigma_3$ and the splitting into even and odd elements is not meaningful.

It is a standard and readily verified fact that

$$\mathbb{C}l_{n+m} \simeq \mathbb{C}l_n \otimes \mathbb{C}l_m,$$  (3.1)

where the tensor product of algebras is in the ‘super’ sense, i.e. with multiplication specified through

$$(x \otimes y)(z \otimes w) = (-1)^{pq}(xz) \otimes (yw),$$

where $y \in \mathbb{C}l_m^p$ and $z \in \mathbb{C}l_m^q$, and $p, q \in \{0,1\}$. 


When $m$ is odd, the Clifford algebra $\mathbb{C}l_m$ has exactly two distinct irreducible representations, each of dimension $2^{(m-1)/2}$, and the image of the (complex) Clifford algebra, in each case, is the entire matrix algebra in the representation space. For example, for $m = 3$, the Pauli matrices give rise to one such representation, with the element $e_j \in \mathbb{C}l_3$ represented by the matrix $\sigma_j$, for $j \in \{1, 2, 3\}$.

As noted before, many of the basic quantum gates are described by means of tensor products of the matrices $\sigma_\alpha$. Since $\otimes^n \mathbb{C}l_3$ is isomorphic to $\mathbb{C}l_3^n$, we may as well view the quantum gate operators as elements of a Clifford algebra $\mathbb{C}l_m$, represented on some finite-dimensional Hilbert space.

Now consider the set $C_m$ consisting of all elements in $\mathbb{C}l_m$ of the form $\pm e_S$, for $S \subset \{1, \ldots, m\}$. Observe that $C_m$ is a group under multiplication (often called the Clifford group), and, furthermore, the square of each element of $C_m$ is $\pm I$. Thus, in the quotient group $V_m = C_m/\{I, -I\}$ the square of every element is the identity and so, in particular, $V_m$ is abelian. It will be convenient to write the group operation in the abelian group $C_m$ additively, even if it is notationally somewhat counter-intuitive. Then we would write the identity element as 0. Because the square of each element is the identity, we have

$$1.x + 1.x = x + x = 0 \quad \text{for all } x \in V_m.$$  

This ensures that $V_m$ is a vector space over the two-element field $\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$.

Let us now consider the projective space $\mathbb{P}(V_m)$ for $V_m$. The points of $\mathbb{P}(V_m)$ are the one-dimensional subspaces of $V_m$. The lines in $\mathbb{P}(V_m)$ are two-dimensional subspaces of $V_m$.

For any $\pm e_S \in C_m$, with $S$ a non-empty subset of $\{1, \ldots, m\}$, we then have a point in $\mathbb{P}(V_m)$; and, conversely, every point of $\mathbb{P}(V_m)$ is a subspace of the form $\{0, \pm e_S\} \subset V_m$, for some non-empty $S \subset \{1, \ldots, m\}$. A line in $\mathbb{P}(V_m)$, being a two-dimensional subspace of $V$, is spanned by two vectors in $V_m$, i.e. it is a subset of $V_m$ of the form $\{0, \pm e_S, \pm e_T, \pm e_S e_T\}$, for two distinct non-empty subsets $S$ and $T$ of $\{1, \ldots, m\}$. Thus, a line in the projective space $\mathbb{P}(V_m)$ is determined by two elements $e_S$ and $e_T$ and contains also a third element corresponding to the product $e_S e_T$.

Thus, we see that the geometry formed by taking as points the elements $\pm e_S$ (one point for the pair $e_S, -e_S$), and taking three points $a, b, c$ to be collinear if the product of two is the third, is precisely the geometry of the projective space $\mathbb{P}(V_m)$.

For $m = 3$ this yields the Fano plane which has seven points and seven lines. This is illustrated in Figure 2 wherein the circular path inside the triangle is one of the seven lines.

It is a general fact that the projective space $\mathbb{P}(V_m)$ (of any vector space $V_m$) satisfies the Desargues property. This explains the observations made by Rau (his Figure 3). An illustration, in terms of Pauli matrices, is in our Figure 3 where
we work with the Clifford algebra $\mathbb{C}l_6 \simeq \mathbb{C}l_3 \otimes \mathbb{C}l_3$ (super-tensor product) and the vertices are labeled up to sign, and we have used the Pauli matrices for a specific representation of $\mathbb{C}l_3$.

We can now state our results formally:

**Proposition 3.1.** Let $P_m$ be the set of all $e_S \in \mathbb{C}l_m$ with non-empty $S \subset \{1, \ldots, m\}$, and let $L_m$ be the set of all triples of distinct elements $a, b, c \in P_m$ such that the
product of two of them is $\pm$ the third. The finite geometry $(P_m, L_m)$ for which $P_m$ is the set of points and $L_m$ the set of lines is a projective geometry isomorphic to the geometry of the projective space $P(Z_m^2)$.

Moreover, if $X$ is the set of points in a projective subspace of $(P_m, L_m)$ then the elements $e_S$ which are in $X$ span a Lie algebra under the bracket commutator.

**Proof.** The first statement in the conclusion has already been proven in the preceding discussion. Now let $X$ be the set of points in a projective subspace of $(P_m, L_m)$. If $e_S$ and $e_T$ are in $X$ then the third point on the line through these points is $\pm e_S e_T$. Now the commutator bracket of $e_S$ and $e_T$ in $C_l m$ is

$$\left[ e_S, e_T \right] = e_S e_T - e_T e_S = (1 - \epsilon_{S,T}) e_S e_T.$$

Thus, the bracket is in the linear span of the elements $e_R \in X$. Therefore, the linear span of $X$ is a Lie algebra.

Rau\cite{Rau2008} shows that certain sets of points give rise to Lie algebras even though they do not form a projective subspace, but rather are Desargues configurations. It is also interesting to note, as Rau points out, that it is possible to decorate the lines of the Fano plane with arrows and, with this decoration, the Fano plane encodes the multiplication of octonions. Since octonion multiplication is not associative, this structure is not the same as that of the Clifford algebra $C_l 3$.

Acknowledgment

My thanks to Bill Hoffman, Ravi Rau, and Neal Stoltzfus for useful discussions. Figure\cite{Figure2} was drawn with Till Tantau’s Ti\kern 0.1667em kZ. I am also thankful to the referee for several constructive suggestions. Research support from US National Science Foundation Grant DMS-0601141 is gratefully acknowledged.

References